KEONTE GATHERS

Cybersecurity / SOC Analyst

Email: keontegathers.kg@gmail.com | LinkedIn: https://www.linkedin.com/in/keonte-gathers/ | GitHub: https://github.com/KeonteGathers

SUMMARY

Cybersecurity/SOC Analyst with hands-on experience in incident response, threat detection, network traffic analysis, digital forensics, and Python automation. Strong background supporting secure workflows, authentication troubleshooting, and sensitive data environments.

CORE SKILLS

Splunk · Wireshark · Suricata · MITRE ATT&CK; · Python · File Integrity Monitoring · Digital Forensics · NIST CSF/800-53 · Risk Assessment

PROJECT HIGHLIGHTS

• Incident Response – Investigated brute-force login attempts and recommended containment.

• Network Traffic Analysis – Identified abnormal TLS patterns indicating potential C2 activity.

• Python Automation – Built SHA-256 File Integrity Monitoring tool.

• USB Forensics – Analyzed registry artifacts and timestamps confirming unauthorized USB activity.

• Risk Assessment – Conducted NIST-based audit identifying gaps and remediation steps.

EXPERIENCE

Department of Social Services — Case Manager Assistant (11/2023–Present)

• Managed confidential case data with secure identity verification.

• Investigated eligibility discrepancies and documented findings.

• Resolved workflow and system access issues.

Independent Contractor — Technical Support & Client Services (01/2019–11/2023)

• Delivered device, network, and account troubleshooting.

• Assisted users with MFA setup, password resets, and secure login recovery.

• Identified unauthorized access attempts and escalated issues.

Wells Fargo — Online Banker (01/2008–01/2019)

• Supported secure online banking access including MFA and password resets.

• Investigated suspicious login attempts and escalated fraud indicators.

• Guided users through secure system navigation.

EDUCATION & CERTIFICATIONS

Google Cybersecurity Professional Certificate (In Progress)

CISSP (In Progress)